Wireshark Traffic Analysis Report

[Anuj kumar, 2301mc04]

October 17, 2025

1 Introduction

This report summarizes the analysis of network traffic captured using Wireshark. The objective was to capture live packets while browsing websites and using the `ping` utility, identify the key protocols involved, and understand their communication patterns.

2 Most Active Protocols

The captured traffic was analyzed using Wireshark's Protocol Hierarchy tool to determine the most active protocols by data volume. The analysis shows that the majority of the traffic was transported over **TCP (58.2%)** and **UDP (38.6%)**.

- **TCP Traffic:** The primary protocol running over TCP was **Transport Layer Security (TLS)**, which is expected from browsing modern `https` websites.
- **UDP Traffic:** A significant portion of UDP traffic was the **QUIC** protocol, which is a modern transport protocol used by many web services (like Google and YouTube) for faster and more efficient communication. **Domain Name System (DNS)** queries, used to resolve website names to IP addresses, also contributed to UDP traffic.

3 Suspicious or Unusual Traffic

No suspicious or unusual traffic was detected during the capture session. All observed activity was directly attributable to the tasks performed:

1. **DNS queries** to resolve the IP addresses of `example.com`, `wikipedia.org`, and other domains.
2. **ICMP traffic** from the `ping 8.8.8.8` command.
3. **TCP, TLS, and QUIC traffic** generated by the web browser to establish secure connections and retrieve website content.

The network communication patterns were normal and expected for standard internet usage.

4 Key Insights about Network Communication

This analysis provided several key insights into standard network operations:

- **DNS as a Prerequisite:** Before any connection to a website can be made, a DNS query must be sent to a DNS server to translate the human-readable domain name (e.g., `www.wikipedia.org`) into a machine-readable IP address.
- **The TCP/TLS Handshake:** For secure web browsing, a client first establishes a reliable connection with the server using the TCP three-way handshake (SYN, SYN-ACK, ACK) on port 443. Immediately following this, a TLS handshake occurs to negotiate encryption protocols and exchange security keys. All subsequent application data (the actual HTTP requests and responses) is then encrypted and sent over this secure TLS tunnel.

- **ICMP for Diagnostics:** The `ping` utility uses the ICMP protocol, which operates independently of web traffic. It provides a simple and effective way to test network connectivity by sending Echo Request packets and waiting for Echo Replies, measuring round-trip time and packet loss.